

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-350784
(43)Date of publication of application : 22.12.1994

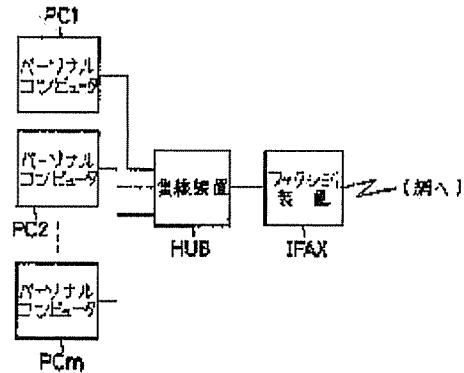
(51)Int.Cl. H04N 1/00
G06F 11/00

(21)Application number : 05-163296 (71)Applicant : RICOH CO LTD
(22)Date of filing : 08.06.1993 (72)Inventor : OSETO FUTOSHI

(54) FACSIMILE EQUIPMENT

(57)Abstract:

PURPOSE: To provide a facsimile equipment in which the infection of a computer virus can be suppressed.
CONSTITUTION: When a file transmitting request is accepted from other personal computers PC1, PC2,..., PCm through a local network, when a floppy disk is mounted on a floppy disk device, and a file is received from the other terminal, whether or not an accepted file, file preserved in the floppy disk, and received file are infected with the computer virus is checked. When they are infected with the computer virus, the file is deleted, or a user is allowed to be informed of the result, so that a situation that the computer virus spreads in the local area network can be sharply suppressed.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-350784

(43)公開日 平成6年(1994)12月22日

(51)Int.Cl.⁵H 04 N 1/00
G 06 F 11/00

機別記号 戸内整埋器号

1 0 6 C 7232-5C
3 1 0 Z

P I

技術表示箇所

審査請求 未請求 請求項の数4 FD (全10頁)

(21)出願番号

特願平5-163296

(22)出願日

平成5年(1993)6月8日

(71)出願人 000006747

株式会社リコー
東京都大田区中馬込1丁目3番6号

(72)発明者 大瀧戸 太

東京都大田区中馬込1丁目3番6号 株式
会社リコー内

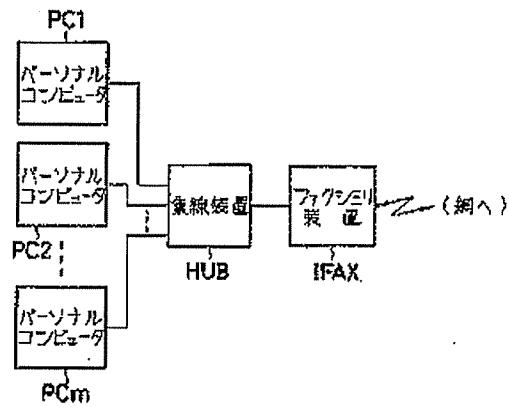
(74)代理人 弁理士 紋田 哉

(54)【発明の名称】 ファクシミリ装置

(57)【要約】

【目的】 コンピュータウイルスの感染を抑制することができるファクシミリ装置を提供することを目的としている。

【構成】 ローカルエリアネットワークを介して、他のパソコンコンピュータPC1, PC2, ..., PCmからファイル送信要求を受け付けたとき、フロッピーディスク装置12にフロッピーディスクが装着されたとき、および、他の端末からファイルを受信したとき、受付ファイル、フロッピーディスクに保存されているファイル、および、受信ファイルが、それぞれコンピュータウイルスに汚染されているかどうかを調べ、汚染されている場合には、そのファイルを消去したり、その旨をユーザに通知するようにしているので、ローカルエリアネットワーク内で、コンピュータウイルスがはびこるような事態を極力抑制することができる。



(2)

特開平6-350784

1

2

【特許請求の範囲】

【請求項1】 少なくとも1つの端末が接続されるローカルエリアネットワークに接続し、このローカルネットワークにおけるローカルエリアネットワークサーバ機能を備えたファクシミリ装置において、

実行可能なファイルおよびデータファイルがコンピュータウイルスに汚染されていることを検出するウイルス検査手段と、

ローカルエリアネットワークに接続されている端末から送信要求されてファイルを受け付けたとき、上記ウイルス検査手段によりその受信したファイルがコンピュータウイルスに汚染されているか否かを判定し、その受信したファイルがコンピュータウイルスに汚染されていることを検出したときは、その受信したファイルを消去する制御手段を備えたことを特徴とするファクシミリ装置。

【請求項2】 少なくとも1つの端末が接続されるローカルエリアネットワークに接続し、このローカルネットワークにおけるローカルエリアネットワークサーバ機能を備えたファクシミリ装置において、

実行可能なファイルおよびデータファイルがコンピュータウイルスに汚染されていることを検出するウイルス検査手段と、

ローカルエリアネットワークに接続されている端末から送信要求されてファイルを受け付けたとき、上記ウイルス検査手段によりその受信したファイルがコンピュータウイルスに汚染されているか否かを判定し、その受信したファイルがコンピュータウイルスに汚染されていることを検出したときは、その受信したファイルを消去するとともに、その旨をその送信要求した端末ユーザに通知する制御手段を備えたことを特徴とするファクシミリ装置。

【請求項3】 少なくとも1つの端末が接続されるローカルエリアネットワークに接続し、このローカルネットワークにおけるローカルエリアネットワークサーバ機能を備えたファクシミリ装置において、

実行可能なファイルおよびデータファイルがコンピュータウイルスに汚染されていることを検出するウイルス検査手段と、

他の端末装置から受信したファイルを蓄積するとともに、上記ウイルス検査手段によりその蓄積したファイルがコンピュータウイルスに汚染されているか否かを判定し、その受信したファイルがコンピュータウイルスに汚染されていることを検出したときは、その受信したファイルを消去する制御手段を備えたことを特徴とするファクシミリ装置。

【請求項4】 少なくとも1つの端末が接続されるローカルエリアネットワークに接続し、このローカルネットワークにおけるローカルエリアネットワークサーバ機能を備えたファクシミリ装置において、

実行可能なファイルおよびデータファイルがコンピュ

タウイルスに汚染されていることを検出するウイルス検査手段と、

他の端末装置から受信したファイルを蓄積するとともに、上記ウイルス検査手段によりその蓄積したファイルがコンピュータウイルスに汚染されているか否かを判定し、その受信したファイルがコンピュータウイルスに汚染されていることを検出したときは、その受信したファイルを消去し、その旨を所定の管理者ユーザに制御手段を備えたことを特徴とするファクシミリ装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、少なくとも1つの端末が接続されるローカルエリアネットワークに接続し、このローカルネットワークにおけるローカルエリアネットワークサーバ機能を備えたファクシミリ装置に関する。

【0002】

【従来の技術】 近年、複数の端末が接続されるローカルエリアネットワークに接続し、このローカルネットワークにおけるファクシミリサーバ機能を実現するファクシミリ装置が実用されている。

【0003】 この場合、このファクシミリ装置に設けられているスキャナ、プリンタ（プロッタ）、および、ファクシミリ通信機能を、ローカルネットワークに接続されている各端末から使用することができ、ローカルエリアネットワークの資源を有効に活用することができる。

【0004】

【発明が解決しようとする課題】 しかしながら、このような従来装置では、次のような不都合を生じていた。

【0005】 すなわち、いわゆるコンピュータウイルスソフトで汚染されたファイルが、ファクシミリ装置を介して外部から侵入し、それにより、ローカルエリアネットワークに接続されているすべての端末に、その侵入したコンピュータウイルスソフトにより感染されるという事態を生じるおそれがある。

【0006】 本発明は、かかる実情に鑑みてなされたものであり、コンピュータウイルスの感染を抑制することができるファクシミリ装置を提供することを目的としている。

【0007】

【課題を解決するための手段】 本発明は、少なくとも1つの端末が接続されるローカルエリアネットワークに接続し、このローカルネットワークにおけるローカルエリアネットワークサーバ機能を備えたファクシミリ装置において、実行可能なファイルおよびデータファイルがコンピュータウイルスに汚染されていることを検出するウイルス検査手段と、ローカルエリアネットワークに接続されている端末から送信要求されてファイルを受け付けたとき、上記ウイルス検査手段によりその受信したファイルがコンピュータウイルスに汚染されているか否かを判定し、その受信したファイルがコンピュータウイルス

(3)

特開平6-350784

3

に汚染されていることを検出したときは、その受信したファイルを消去する制御手段を備えたものである。

【0008】また、少なくとも1つの端末が接続されるローカルエリアネットワークに接続し、このローカルネットワークにおけるローカルエリアネットワークサーバ機能を備えたファクシミリ装置において、実行可能なファイルおよびデータファイルがコンピュータウイルスに汚染されていることを検出するウイルス検査手段と、ローカルエリアネットワークに接続されている端末から送信要求されてファイルを受け付けたとき、上記ウイルス検査手段によりその受信したファイルがコンピュータウイルスに汚染されているか否かを判定し、その受信したファイルがコンピュータウイルスに汚染されていることを検出したときは、その受信したファイルを消去するとともに、その旨をその送信要求した端末ユーザに通知する制御手段を備えたものである。

【0009】また、少なくとも1つの端末が接続されるローカルエリアネットワークに接続し、このローカルネットワークにおけるローカルエリアネットワークサーバ機能を備えたファクシミリ装置において、実行可能なファイルおよびデータファイルがコンピュータウイルスに汚染されていることを検出するウイルス検査手段と、他の端末装置から受信したファイルを蓄積するとともに、上記ウイルス検査手段によりその蓄積したファイルがコンピュータウイルスに汚染されているか否かを判定し、その受信したファイルがコンピュータウイルスに汚染されていることを検出したときは、その受信したファイルを消去する制御手段を備えたものである。

【0010】また、少なくとも1つの端末が接続されるローカルエリアネットワークに接続し、このローカルネットワークにおけるローカルエリアネットワークサーバ機能を備えたファクシミリ装置において、実行可能なファイルおよびデータファイルがコンピュータウイルスに汚染されていることを検出するウイルス検査手段と、他の端末装置から受信したファイルを蓄積するとともに、上記ウイルス検査手段によりその蓄積したファイルがコンピュータウイルスに汚染されているか否かを判定し、その受信したファイルがコンピュータウイルスに汚染されていることを検出したときは、その受信したファイルを消去し、その旨を所定の管理者ユーザに制御手段を備えたものである。

【0011】

【作用】したがって、ファクシミリ装置を介してローカルエリアネットワークの内外でやりとりされるファイルのすべてについて、コンピュータウイルス感染の状況を検出でき、感染ファイルは消去しているので、コンピュータウイルス感染の影響を大幅に抑制することができる。

【0012】

【実施例】以下、添付図面を参照しながら、本発明の実

4

施例を詳細に説明する。

【0013】図1は、本発明の一実施例にかかるローカルエリアネットワークシステムを示している。

【0014】同図において、m台のパーソナルコンピュータPC1、PC2、・・・、PCmと、ローカルエリアネットワークサーバ機能を備えたファクシミリ装置1FAXは、集線装置HUBに接続され、この集線装置HUBを介して、これらのパーソナルコンピュータPC1、PC2、・・・、PCmおよびファクシミリ装置1FAXが接続されている。

【0015】ここで、集線装置HUBは、例えば、10BASE-T(IEEE802.3CSMA/CD)などのスター型のローカルエリアネットワークを構成するためのものである。また、このローカルエリアネットワークシステムでは、おのおののパーソナルコンピュータPC1、PC2、・・・、PCm、および、ファクシミリ装置1FAXの制御処理やアプリケーションソフトウェアのプログラムは、いわゆるマルチウインド型のネットワーク・オペレーティング・システムを基礎にしている。また、このローカルエリアネットワークシステムには、それを管理するための管理者ユーザが、一人以上設定されている。

【0016】また、ファクシミリ装置1FAXには、パーソナルコンピュータPC1、PC2、・・・、PCmと同じ1つ以上のアプリケーションソフトウェア、または、それらのアプリケーションソフトウェアで作成されたファイルを印刷可能なアプリケーションプログラムがインストール(実装)されている。それとともに、このファクシミリ装置1FAXは、アプリケーションソフトウェアで作成されているファイルデータの送受信機能を備えている。

【0017】図2は、ファクシミリ装置1FAXの一例を示している。

【0018】同図において、CPU(中央処理装置)1は、このファクシミリ装置1FAXの各部の動作制御、グループ3ファクシミリ伝送機能、および、ローカルエリアネットワークサーバ機能の処理を実現するためのものであり、ROM(リード・オンリ・メモリ)2は、CPU1が実行する処理で参照する各種データやこのファクシミリ装置1FAXに固有な情報(例えば、後述する機体識別番号など)を記憶するためのものであり、RAM(ランダム・アクセス・メモリ)3は、CPU1の主記憶やワークエリアなどを構成するためのものであり、時計装置4は、現在時刻情報を出力するためのものである。RAM3と時計装置4は、バッテリ5によってバックアップされている。

【0019】スキャナ6は、所定の解像度で原稿画像を読み取り入力するためのものであり、画像処理部7は、スキャナ6の動作を制御するとともに、スキャナ6で読み取って得た画像データに対して、画素密度変換などの

56

(4)

特開平6-350784

5

種々の画像処理を適用するものである。

【0020】ページプリンタ8は、レーザビームプリンタなど、普通紙に高解像度で高画質の画像を記録するためのものであり、記録制御部9は、ページプリンタ8の記録動作を制御するためのものである。

【0021】操作表示部10は、このファクシミリ装置1FAXをローカルに直接操作するためのものであり、符号化復号化部11は、所定の画像符号化／復号化処理を実行するためのものである。

【0022】フロッピーディスク装置12は、フロッピーディスク（図示略）にデータを記録／再生／消去するためのものであり、フロッピーディスク制御部13は、フロッピーディスク装置12の動作を制御するためのものである。

【0023】磁気ディスク装置14は、大容量の外部記憶装置であり、システムソフトウェア、システムファイル、コンピュータウイルス検出ソフトなどの複数のアプリケーションソフトウェア、多数の画像ファイル、および、アプリケーションソフトファイルデータなどが記憶される。また、磁気ディスク制御部15は、磁気ディスク装置14の動作を制御するためのものである。

【0024】ローカルエリアネットワークインターフェース16は、集線装置HUBに接続するためのものであり、ローカルネットワーク制御部17は、所定のローカルエリアネットワーク制御手順にしたがったデータ伝送動作を実行するためのものである。

【0025】グループ3ファクシミリモデム18は、グループ3ファクシミリのモデム機能を実現するためのものであり、伝送手順信号をやりとりするための低速モデム機能（V. 21 モデム）、および、ねもに画像情報をやりとりするための高速モデム機能（V. 33 モデム、V. 29 モデム、V. 27ter モデムなど）を備えている。

【0026】調制御装置19は、このファクシミリ装置1FAXを公衆電話回線網に接続するためのものであり、自動発着信機能を備えている。また、この調制御装置19には、通話のためのハンドセット20が付設されている。

【0027】これらのCPU1、ROM2、RAM3、時計装置4、画像処理部7、記録制御部9、操作表示部10、符号化復号化部11、フロッピーディスク制御部13、磁気ディスク制御部15、ローカルエリアネットワーク制御部17、グループ3ファクシミリモデム18、および、調制御装置19は、システムバス21に接続されており、これらの各要素間のデータのやりとりは、主としてこのシステムバス21を介して実行される。

【0028】図3は、ローカルエリアネットワークを介して、他のパソコンコンピュータPC1、PC2、…、PCmからファイル送信要求を受け付けるときの

6

ファクシミリ装置1FAXの処理例を示している。

【0029】いずれかのパソコンコンピュータPC1、PC2、…、PCmより、ファイル送信が要求されると、ファクシミリ装置1FAXは、そのファイル送信要求を受け付けて（処理101）、そのファイル送信要求を発行したパソコンコンピュータPC1、PC2、…、PCmから、送信対象となるファイル（以下、受付ファイルという）を受信して、その受信した受付ファイルを保存する（処理102）。

10 【0030】そして、コンピュータウイルス検査ソフトを起動して、その受付ファイルがコンピュータウイルスに汚染されているかどうかを調べる（処理103、判断104）。判断104の結果がYESになるときには、その受付ファイルを消去して（処理105）、そのときに送信要求したユーザがログインしているパソコンコンピュータPC1、PC2、…、PCmに対して、受付ファイルがコンピュータウイルスに汚染されていたためにそのファイルを消去して、送信受付を解除した旨を通知するメッセージを送信して（処理106）、この処理を終了する。

20 【0031】また、受付ファイルがコンピュータウイルスに汚染されていない場合で、判断104の結果がNOになるときには、そのときに指定された宛先を発呼して、そのときの受付ファイルを送信する送信処理を実行し（処理107）、この処理を終了する。

【0032】図4は、フロッピーディスク装置12にフロッピーディスクが装着されたときに実行する処理を示している。

30 【0033】まず、フロッピーディスクに保存されているファイルを1つ選択し（処理201）、コンピュータウイルス検査ソフトを起動して、その選択ファイルがコンピュータウイルスに汚染されているかどうかを調べる（処理202、判断203）。判断203の結果がYESになるときには、その選択ファイルをウイルス汚染ファイルに設定し（処理204）、判断203の結果がNOになるときには、その選択ファイルをウイルス非汚染ファイルに設定する（処理205）。

40 【0034】このようにして、1つのファイルについてコンピュータウイルス汚染状況を判断すると、すべてのファイルに対する処理が終了したかどうかを調べて（判断206）、判断206の結果がNOになるときには、処理201に戻り、残りのファイルについての処理を実行する。

【0035】また、判断206の結果がYESになるときは、そのときの検査結果の一覧表時を、操作表示部10に表示して（処理207）、この処理を終了する。

【0036】図5は、このファクシミリ装置1FAXが着信検出したときの処理例を示している。

50 【0037】着信検出すると、着信応答して（処理301）、所定の受信処理を実行し（処理302）、そのと

(5)

特開平6-350784

7

きに受信したファイルを一時保存する。そして、コンピュータウイルス検査ソフトを起動して、その受信ファイルがコンピュータウイルスに汚染されているかどうかを調べる(処理303、判断304)。

【0038】判断304の結果がYESになるときは、その受信ファイルを消去して(処理305)、所定の管理者ユーザがログインしているパソコンコンピュータPC1、PC2、…、PCmに対し、受信ファイルがコンピュータウイルスに汚染されていたためにそのファイルを消去した旨を通知するメッセージを送信して(処理306)、この処理を終了する。

【0039】また、受信ファイルがコンピュータウイルスに汚染されていない場合で、判断307の結果がNOになるときには、そのときの受信ファイルがコンピュータウイルス検査ソフトであるかどうかを調べる(判断307)。判断307の結果がYESになるときには、そのときの受信ファイルを磁気ディスク装置14のアプリケーション領域に登録して(処理308)、この処理を終了する。

【0040】また、判断307の結果がNOになるときには、所定の管理者ユーザがログインしているパソコンコンピュータPC1、PC2、…、PCmに対し、ファイルを受信した旨をあらわすメッセージを送信して(処理309)、この処理を終了する。

【0041】このようにして、本実施例では、ローカルエリアネットワークを介して、他のパソコンコンピュータPC1、PC2、…、PCmからファイル送信要求を受け付けたとき、フロッピーディスク装置12にフロッピーディスクが装着されたとき、および、他の端末からファイルを受信したとき、受付ファイル、フロッピーディスクに保存されているファイル、および、受信ファイルが、それぞれコンピュータウイルスに汚染されているかどうかを調べ、汚染されている場合には、そのファイルを消去したり、その旨をユーザに通知するようにしてるので、ローカルエリアネットワーク内で、コンピュータウイルスがはびこるような事態を極力抑制することができる。

【0042】ところで、上述した実施例では、ローカルエリアネットワークに接続されるファクシミリ装置FAXについて、本発明を適用した場合について説明したが、本発明は、図6に示すように、1つのパソコンコンピュータPCに接続されているファクシミリ装置FAX'についても、同様にして適用することができる。

8

【0043】この場合、ファクシミリ装置FAX'は、図7に示したように、図2に示したファクシミリ装置FAXのローカルエリアネットワークインターフェース16およびローカルネットワーク制御部17を、パソコンコンピュータPCに接続するためのホストインターフェース回路22に置き換えた構成をもつ。また、このファクシミリ装置FAX'も、上述したファクシミリ装置FAXと同様の送受信機能を備える。

【0044】また、卓体のファクシミリ装置についても、本発明を同様にして適用することができる。

【0045】なお、本発明は、上述した構成と異なるシステム構成のファクシミリ装置についても同様にして適用することができ、また、グループ4ファクシミリ装置についても、本発明を同様にして適用することができ

る。

【0046】

【発明の効果】以上説明したように、本発明によれば、ファクシミリ装置を介してローカルエリアネットワークの内外でやりとりされるファイルのすべてについて、コンピュータウイルス感染の状況を検出でき、感染ファイルは消去しているので、コンピュータウイルス感染の影響を大幅に抑制することができるという効果を得る。

【図面の簡単な説明】

【図1】本発明の一実施例にかかるローカルネットワークシステムの一例を示したブロック図。

【図2】本発明の一実施例にかかるファクシミリ装置の一例を示したブロック図。

【図3】ローカルエリアネットワークを介してパソコンコンピュータからファイル送信要求を受け付けるときのファクシミリ装置の処理例の一部を示したフローチャート。

【図4】フロッピーディスク装置にフロッピーディスクが装着されたときの処理例を示したフローチャート。

【図5】着信検出時の処理例を示したフローチャート。

【図6】本発明の他の実施例にかかるシステムの一例を示したブロック図。

【図7】本発明の他の実施例にかかるファクシミリ装置の一例を示したブロック図。

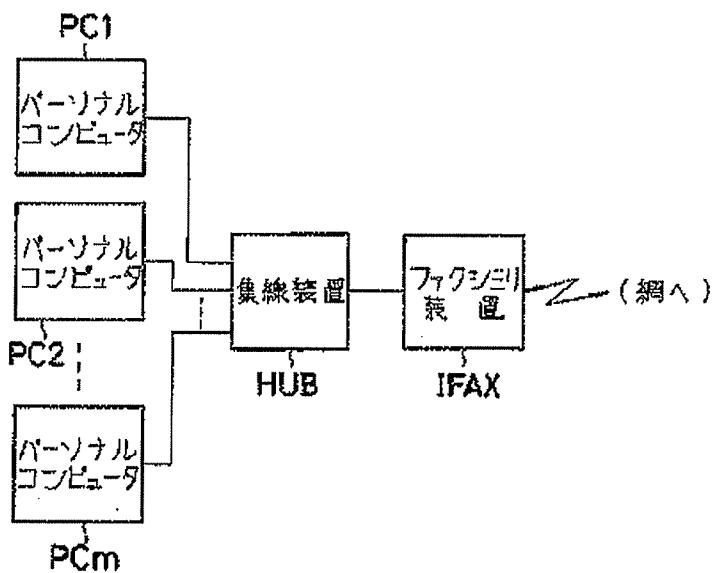
【符号の説明】

PC1～PCm、PC パソコンコンピュータ
HUB 集線装置
FAX、FAX' ファクシミリ装置

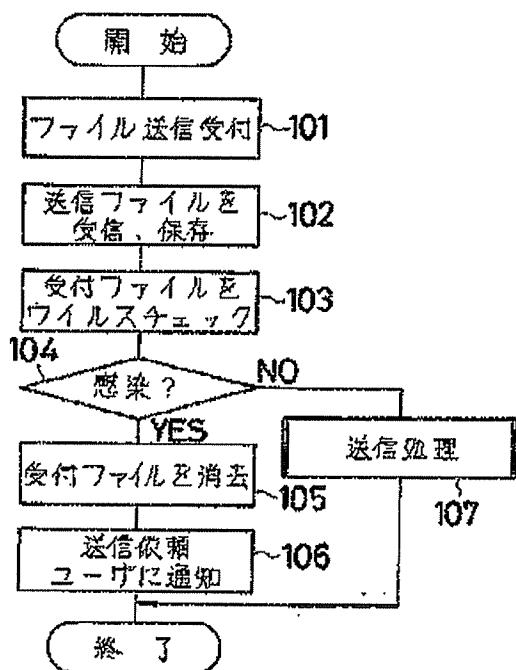
(6)

特開平6-350784

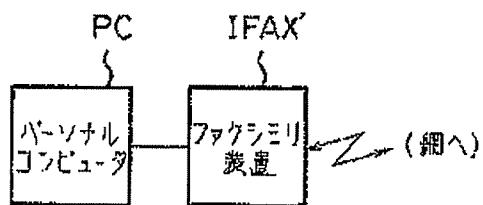
【図1】



【図3】



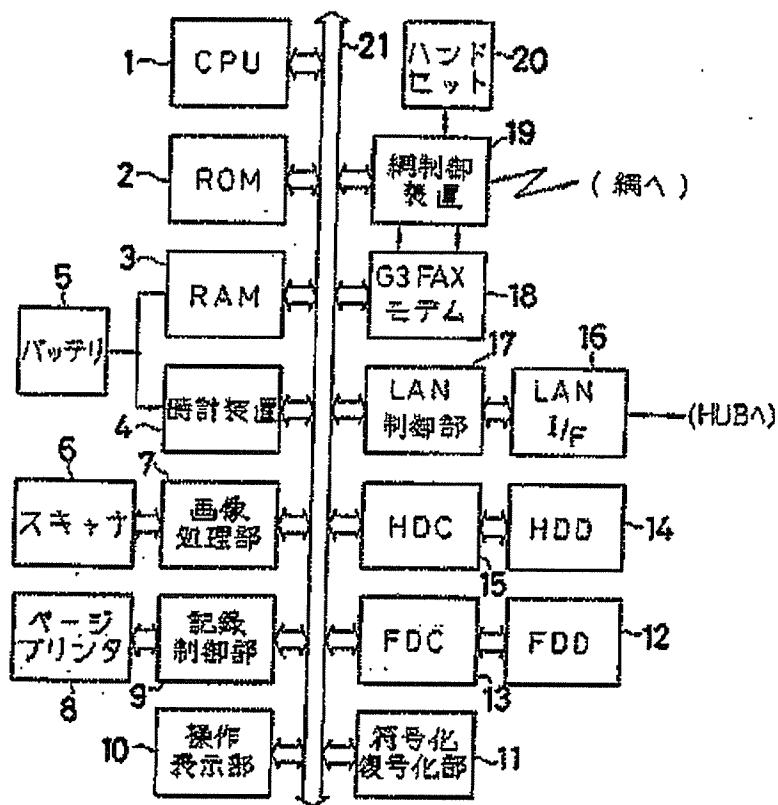
【図6】



(7)

特開平6-350784

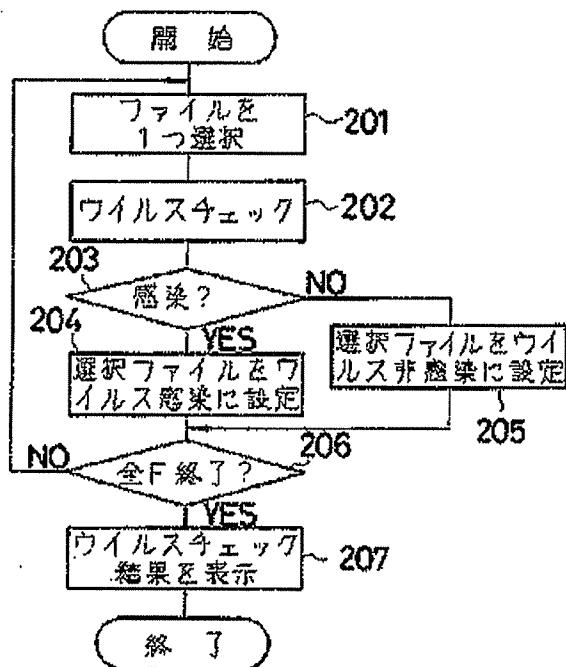
【図2】



(8)

特開平6-350784

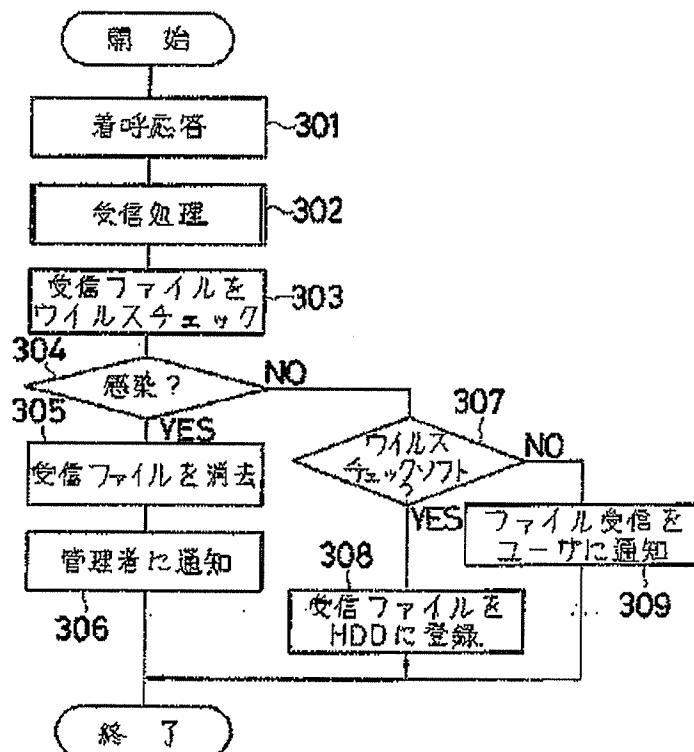
【図4】



(9)

特開平6-350784

[図6]



(10)

特開平6-350784

【図7】

